International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 1522–1539

# Multi-perspective DOS Attack Detection Framework for Reliable Data Transmission in Wireless Sensor Networks based on Trust Factor

Dr. D. Stalin David [1], D. Saravanan[2]

*Assistant Professor[1], Department of CSE, IFET College of Engineering, Villupuram,*
*Associate Professor[2], Department of CSE, IFET College of Engineering, Villupuram,*
*Email: sdstalindavid707@gmail.com[1], saranmds@gmail.com2*

***Abstract***

*Wireless sensor networks are considered to be used in a variety of applications that require wireless networks to collect data and transmit data. However, with its main limitations of resource constraints, the deployment of WSN in an unattended and critical scenario makes it vulnerable to network security threats. In particular, by selectively dropping packets, selective forwarding degrades the network performance and the hello flood attack is also responsible for flooding a large number of hello request packets over the network 's real nodes, resulting in reduced sensor node availability. In this paper, the Reliable Data Transmission Multi-perspective Trust Factor-based DOS Attack Detection Framework (MTF-DOSADF) proposed to counteract two DOS attacks such as selective forwarding and hello flood attacks in order to maintain maximum performance of the degree of network cooperation. Through the extraction and estimation of multi-dimensional confidence parameters that determine the reliability of sensor nodes in packet forwarding activity, this proposed MTF-DOSADF plays a vital role in accurately detecting DOS attacks. The simulation experiments of the proposed MTF-DOSADF confirmed an improvement rate of 13 percent in throughput and 18 percent reduced energy consumption compared to the current DOS attack detection framework considered for investigation, with 21 percent reduced packet latency.*

***Keywords:*** *Wireless Sensor networks, DOS Attack, Selective Forwarding, Hello Flood Attacks, Multi-perspective Trust Factor.*

## 1. Introduction

Wireless Sensor Networks ( WSNs) have been considered to be the most interesting and promising domain in recent decades due to their ability to aggregate data and investigate data, making it highly suitable for monitoring and monitoring real-time applications[1]. They use WSN in military, civilian, environmental and fleet monitoring due to real-time implementation. Due to the energy resources and memory requirements of WSNs[2], traditional security approaches are considered to be less appropriate. In addition, the sensor nodes incorporate the advantages of multi-hop data transmission for the transmission of the packets to the base station as they are restricted by a limited range of transmission [3]. Therefore, for maximum and reliable data dissemination in the network[4], The potential for packet forwarding of sensor nodes and their co-operation capabilities attributed to other interacting sensor nodes are crucial. A malicious opponent, however, has the ability to launch attacks on the sensor networks, since they are potentially carried out in hostile environments[5]. Selective forwarding and hello flood attacks, in particular, belong to the category of DOS attacks caused by the network's internal malicious sensor nodes. The Selective forwarding attack is a particular type of DOS attack in which sensor nodes either forward or drop a selective number of packets forwarded to the base station of the network by the other interacting sensor nodes[6]. Similarly, another type of DOS attack is a hello flood attack that deliberately induces a malicious node to generate huge numbers of hello requests that the network's cooperating sensor nodes

ISSN: 2233-7857 IJFGCN

could not handle[7]. In order to facilitate the process of cooperation and collaboration in the network, these selective forwarding and hello flood attacks thus disturb the rate of packet delivery and the availability of sensor nodes.

In this paper, the Multi-perspective Trust Factor-based DOS Attack Detection Framework (MTF-DOSADF) helps detect and manage the effects of internal attacks such as selective forwarding and hello flood attacks to maintain the extent of network collaboration to maximize network performance. The mitigation of selective forwarding is facilitated by the estimation of the reputation factor determined on the basis of the extraction of network parameters such as energy, packet forwarding potential, in this proposed MTF-DOSADF framework.

Similarly, by determining the availability factor, the effect of the hello flood attacks is mitigated. The simulation experiments of the proposed MTF-DOSADF framework are also carried out by varying the number of sensors and malicious nodes of the network using evaluation metrics such as packet dissemination rate, energy consumption, packet latency and reliable detection rate.

The remaining sections are structured as follows in the paper. Section 2 presents a literature survey of the most recent defense mechanisms that have helped counteract the impact of selective forwarding and hi-flood attacks on sensor networks. With its integrated estimate of multi-perspective factors that decide the existence of selective forwarding and hello flood attacks in sensor networks, section 3 describes the detailed view of the proposed MTF-DOSADF framework. Section 4 describes the simulation details and outcome inferences of the proposed MTF-DOSADF framework quantified by varying the number of sensors and malicious network nodes using packet dissemination rate, energy consumption, packet latency and reliable detection rate. With major contributions and possible scope of future research, Section 5 concludes the paper.

## 2. Related Work

A reliable defence mechanism using the Support Vector Machine (SVM) was initially proposed to isolate the impact of selective malicious node forwarding from the sensor networks[11]. By incorporating an IDS that helped detect a specific spectrum of DOS attacks based on the derivation of hop count and bandwidth from the network, this SVM-based defence approach is appropriate for a simple classification approach. In order to avoid the problem of over fitting that reduces the effects of dimensionality reduction, this SVM-based defense approach was determined. For the maintenance of the lifetime of the sensor nodes with reduced energy consumption in the network[12], a node location determination approach for handling selective forwarding nodes was contributed. A mean detection rate of 90.64 percent with a reduced false negative rate and a positive rate of 13.62 percent and 32.63 percent respectively were confirmed by this node location determination approach. Then, using the merits of Location Dependent Key Management Technique[13], an RSS and distance-based defense mechanism of hello flooding attack was proposed. This Location Dependent Key Management Technique does not require node location information to ensure superior connectivity for the effective detection of hello flooding attack nodes in the network, so it plays a very high level of connectivity.

In addition, using multiple layers to facilitate anomaly detection by incorporating rule processing and MAC pooled ID[14], an efficient Selective Forwarding Detection Approach was proposed. This Selective Forwarding Detection Approach was proposed to maintain the degree of security during the process of data transmission allowed between the base station and the source sensor nodes of the network. In malicious node detection processes, this Selective Forwarding Detection Approach has been shown to be scalable, energy efficient and reliable. In order to improve the rate of packet dissemination in the network, a neighborhood-based detection system was proposed to mitigate the selective forwarding attack

ISSN: 2233-7857 IJFGCN

and the hello flooding attack[15]. The merits of the Alpha and Beta-based flexible filtering scheme were used by this Neighborhood-based detection system to effectively detect malicious sensor nodes in the network. This Neighborhood-based detection system facilitates a low false positive rate and maximised detection precision. It was also determined that collusion attack can be detected in such a way that the packet dropping rate can be reduced to the maximum degree in the network. An Enhanced Detection Approach was proposed to enhance the quality of service and energy conservation in the network by reliably detecting the presence of a selective forwarding attack on the network[16].

In addition, an Active Defence Approach was proposed to understand the influence of the Selective Forwarding attack on the network during the use of the LEACH protocol[17]. In the effective detection process of the selective forwarding attack under LEACH protocol routing, the optimal energy factor was considered. In order to reduce the rate of packet drop, this Active Defence Approach was concluded with energy consumption in the network independent of the number of malicious nodes existing in the network. An enhanced reputation-based Active Trust-based DOS Attack Detection Framework (IRA-DOSDF) was proposed through the benefits of a dual-stage security approach that focuses on the process of securing and selecting data packets for efficient data dissemination[18].

Highly focused on mitigating specific types of data routing attacks such as a black hole and selective forwarding attack that introduces maximum packet drop in the network, this IRA-DOSDF framework The cuckoo search algorithm was used by this IRA-DOSDF framework for confidence path determination and optimization that maintains the use of energy in the network in a predominant way. The IRA-DOSDF framework was confirmed to extend the lifespan of the network with probabilistic investigation of the extracted parameters during the analysis. In addition, a Hybrid DOS attack detection framework (ET-HDOSDF) based on Energy Trust was proposed to increase the detection rate in selective forwarding and hello flooding attacks on the network[19]. A series of energy correlation checks were included in this ET-HDOSDF framework to confirm the existence of selective forwarding and hi-flooding attacks in the network. With the minimized impact of Hybrid DOS attack on the considered network traffic considered in the detection process, this ET-HDOSDF framework was estimated to extend the network lifetime. Finally, for potential detection of both selective forwarding and hello flooding attacks, an Enhanced Gradient Routing-based DOS attack Detection Framework (EGR-DOSDF) was proposed in order to extend the lifetime of the network[20]. The gradient computation was used to locate the malicious nodes in the network using this EGR-DOSDF framework. With highly reduced packet latency and energy consumption, the throughput, packet dissemination ratio of this EGR-DOSDF framework has been concluded to be the maximum. Various trust-assurance techniques, fault identification, estimation of sensor location, secure link formation and confidence assurance among the nodes are shown. WSN 's review of congestion control, confidence assurance, and fault detection addresses the issues of power consumption, link breaches due to the incorrect propagation of information between the nodes, and the description of unique features. The main consideration in the WSN design is the maintenance of a low false alarm ratio with rapid detection of patient abnormalities. The decision tree architecture is integrated with the linear regression formula for effective anomaly detection in order to meet these limitations. However, the lack of support for mobility and the dynamic route adjustments are still investigating the parameters of the confidence assessment mechanism.

The high vulnerability of the trust management system to the number of attacks has been ignored by traditional trust mechanisms. This limitation transforms the research work into a two-tier resistant attack architecture and trust management systems. The incorporation of the Collection Tree Protocol (CTP) with the trust management system provides a trade-off between detection of high security and malicious behaviour. The cross-layer WBAN (MAC frame and PHY frame) architectural framework suffers from major challenges in the generation of new protocols that require optimised solutions. The

ISSN: 2233-7857 IJFGCN

MAC framework is integrated with the energy harvesting architecture and power positional authority inclusion in order to increase the lifetime of a network. Due to resource constraints and heterogeneous features, the authentication schemes seem to be as inefficient form. Certificate and certificate-less protocols have been developed in research studies that address the issues of security provision at the application level. In cryptographic algorithms, key management complications for users and data owners are greater. For this, the multiple data owner scenarios and the user division in multiple security domains reduce the complexities of key management and achieve fine-grained access control. To decrypt messages, the attributes related to the cipher text must satisfy the access control structure.

## 3. Proposed Multi-perspective DOS Attack Detection Framework (MTF-DOSADF) based on Trust Factor (MTF)

Four modules are used in the proposed MTF-DOSADF framework: a) Multiple Network Parameters Extraction Module, b) Node Behavior Monitoring Module, c) Reputation and Availability Factor Estimation Module and d) Mitigation Module for Selective Forwarding and Hello Flooding Attack. The detailed process included in each of the modules of the proposed framework for the MTF-DOSADF is presented as follows.

### *3.1 Multiple Network parameters Extraction Module*

Multiple Network Parameters The Extraction Module may be responsible for extracting network parameters to help determine the malicious intent of the network sensor nodes. The potential factors of each sensor node, such as packet forwarding potential, throughput, data rate, hop count, and energy consumption, are extracted from the network. In order to detect the presence of a Selective Forwarding attack, the parameters mentioned above, such as energy consumption, throughput and packet forwarding potential, are necessary. For Hello Flooding Attack detection, parameters such as packet forwarding potential, data rate and hop count are vital.

### *3.2 Node Behavior Monitoring Module*

The node parameters are monitored in this Node Behavior Monitoring Module either through direct monitoring or neighborhood monitoring to estimate the degree of reputation that determines the compromise of selective forwarding attack and the availability factor to detect the existence of Hello Flooding Attack.

ISSN: 2233-7857 IJFGCN

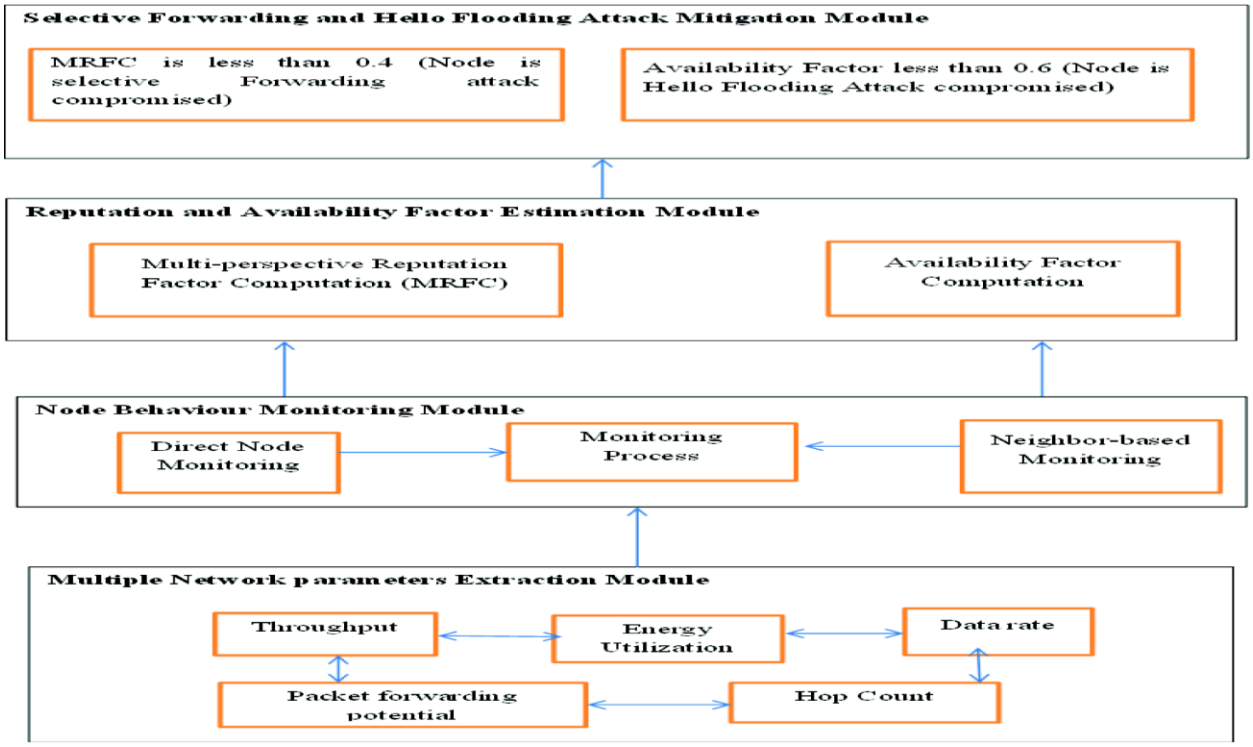


**Figure 1: Architecture of the proposed MTF-DOSADF Framework**

### *3.3 Factor Estimation Module for Reputation and Availability*

In this module, two variables are calculated on the basis of the details below, such as Multi-perspective Reputation Factor Computation (MRFC) and Availability Factor (AF).

### *3.4 Multi-perspective Computation of Reputation Factor (MRFC) Computation*

The MRFC calculation is facilitated by the inclusion of three steps: I Connotative Trust and Instinctive Reputation Estimation, ii) Factor Trust Parameter (FTP) and Malicious Grading Factor (MGF) Determination, and iii) MRFC estimation by integrating FTP and MGF. The main focus of this computing process is to detect the existence of a selective forwarding attack on the network, as reputation and trust are considered to be the best approach for detecting such attacks.

### *3.5 Estimation of Connotative Trust and Instinctive Reputation*

Connotative Trust is considered to be the type of subjective trust of sensor nodes determined by the monitoring process enabled through direct observation accumulated over a period of time based on the neighbourhood sensor nodes of the network. Based on the interaction period, this Connotative Trust helps judge the trust held by each of the sensor nodes. This Connotative Trust helps to quantify the degree of cooperation attributed to each sensor node in terms of packet forwarding potential towards the other directly interacting sensor nodes of the network. In particular, if a sensor node is examined to evaluate its Connotative Trust,

$$Conn\_Trust(s_i, s_j)_{(t)} = Act\_Trust(s_i, s_j) \text{ if } \left| Act\_trust(s_i, s_j) - Avg\_trust(n_i) \right| \le \alpha \quad (1)$$

$$Conn\_Trust(s_i, s_j)_{(t)} = Act\_trust(s_i, s_j) + \frac{Act\_trust(s_i, s_j) - Avg\_trust(s_i)}{\sum_{k=1}^{M(N)} \left| Act\_trust(s_i, s_k) - Avg\_trust(s_i) \right|} \text{ if}$$

$$\left| Act\_Trust(s_i, s_j) - Avg\_Trust(s_i) \right| \le \alpha \quad (2)$$

ISSN: 2233-7857 IJFGCN

Then, using Equation ( 3), the threshold used to assess the level of Connotative Trust associated with each sensor node is determined.

$$\alpha = \sqrt{\frac{\sum_{k=1}^{O(n_i)} (Act\_Trust(s_i, s_j) - Avg\_Trust(s_i)^2}{O(M_{SN})}} \quad (3)$$

### *3.6 Determination of Factor Trust Parameter (FTP) and Malicious Grading Factor (MGF)*

The Factor Trust Parameter (FTP) is then determined on the basis of the feasible possibility of predicted agreement between multiple Equation-computed observing nodes (4)

$$\hat{M}_{A(ME)} = \sum_{j=1}^{K_m} M^2_{A(MO(j))} \quad (4)$$

However, there are two significant limitations to the traditional Fleiss Kappa statistical reliability factor (dependence on marginal distribution) and they need to be addressed by calculating improved S-statistics for malicious grading factor (MGF) using equation ( 5)

$$M^*_{A(ME)} = \frac{\sum_{j=1}^{K_m}\sum_{k=1}^{K_m}(P_{W(ik)} r_{ij} r_{jk} - r_j)}{r_i(r_i - 1)} \quad (5)$$

With the probability weight parameter determined through Equation (6)

$$P_{W(jk)} = 1 - \frac{|j-k|}{(K_m - 1)} \quad (6)$$

### *3.7MRFC estimation by integrating FTP and MGF*

Finally, the MRFC factor is determined on the basis of the standard deviation derived from the mean degree of observation accumulated using Equation ( 7) over FTP and MRF, respectively.

$$MRFC(SN_{(i)}) = \frac{M_{A(ME)} - \hat{M}_{A(ME)}}{1 - \hat{M}_{A(ME)}} \quad (7)$$

With the values of $M_{A(ME)}$ and $\hat{M}_{A(ME)}$ determined based on Equations (8) and (9) respectively

$$M_{A(ME)} = \frac{1}{N_m} \sum_{i=1}^{N_m} M^*_{A(ME)} \quad (8)$$

$$M_{A(ME)} = \frac{1}{N_m} \sum_{i=1}^{N_m} M^*_{A(ME)} \quad (9)$$

ISSN: 2233-7857 IJFGCN

Therefore, the MRFC factor helped to identify the sensor nodes that were compromised by a selective network forwarding attack.

### *3.8Estimation of Availability Factor*

The advantages of Fleiss Kappa for determining the degree of trust and availability potential rendered by the sensor nodes of the network under routing are derived from this estimation of the availability factor that helps to detect hello flooding attack. Let each sensor node among the $N_m$ nodes are monitored by $K_m$ neighbors in the network. The traditional statistical reliability factor of Fleiss Kappa is then potentially used to generalize the incorporation of kappa statistics in order to classify the monitored node into a genuine hello flooding attack. The classical Fleiss Kappa statistical reliability factor is primarily used because multiple monitoring nodes monitor the sensor nodes. The Fleiss Kappa statistical reliability factor of the monitored sensor nodes '$i$' that classifies it into a specific category of ordinal scale '$j$' (selfish and genuine) is derived using Equation (10)

$$FK_{RF(ij)} = \frac{r_{ij}(r_{ij}-1)}{2} \qquad (10)$$

Where $FK_{RF(i)} = \sum_{j=1}^{K_m} FK_{RF(j)}$ represents the number of multiple observers that have designated mobile nodes into the same ordinal scale of categorization.

Then the mean agreement between the multiple observers about the specific sensor nodes '$i$' is derived using Equation (11)

$$\hat{M}_{A(MO)} = \frac{1}{N_m}\sum_{i=1}^{N_m} M_{A(MO(i))} \quad (11)$$

with the cumulative estimation related to a sensor node rated by a multiple number of observers is computed using Equation (12)

$$M_{A(MO(i))} = \frac{2FK_{RF(i)}}{r_i(r_i-1)} \quad (12)$$

In addition, the proportion of expectation manipulated for grading the sensor nodes into hello flooding attacked and genuine (Availability Factor (AF)- $FK_{RFC(i)}$ ) is derived through Equation (13)

$$FK_{RFC(i)} = \frac{\hat{M}_{A(MO)} - \hat{M}_{A(ME)}}{1-\hat{M}_{A(ME)}} \quad (13)$$

This Availability Factor aids in determining a specific sensor nodes as the Hello Flooding Attackcompromised.

### *3.9Selective Forwarding and Hello Flooding Attack Mitigation Module*

Compared with the detection thresholds of 0.4 and 0.6 (determined based on simulations), the computed multi-perspective reputation factor computation (MRFC) and computed availability factor are compared in this final module. Sensor nodes with MRFC and AF below 0.4 and 0.6 are therefore isolated from the network to achieve a maximum data dissemination rate in order to extend the life of the network.

ISSN: 2233-7857 IJFGCN

### *3.10 Energy Consumption Model*

The following energy consumption model for energy calculation in wireless sensor networks is utilized. The various parameters used are shown in table 1

**Table 1** Energy Consumption Model

| Operation | Energy Dissipated |
|---|---|
| Transmitter Electronics (ETx-elec)<br>Receiver Electronics (ERx-elec)<br>(ETx-elec = ERx-elec = Eelec) | 50 nJ/ bit |
| Transmitter Amplifier ( amp) | 100 pJ/ bit/ m2 |
| To transmit a message of size k-bits,<br>over distance *d* m | ETx(k, d) = Eelec × k + amp × k × d |
| To receive a k-bit message | ERx(k) = Eelec×k |
| Cost for data fusion | 5 nJ/ bit/ message |

According to this model, each sensor node's transmitter electronics function at 50 nJ per bit sent. With reference to bits received, the same is true for receiver electronics. 100pJ / bit / m2 will be required to amplify the signal sent by the transmitter, and the radio will be shut down during down time to prevent unwanted message reception. Therefore, the total transmission cost of k bits over a distance d will be regulated by the equation.

$$E_{Tx}(k,d)=(E_{elec}\times k)+(E_{amp}\times k\times d^2) \quad (14)$$

Whereas the cost of receiving and aggregating the data from n senders will be governed by the following equations:

$$E_{Rx}(k)=(Eelec\times k),n=1 \quad (15)$$

$$E_{Da}(k)=(5\times k\times n),n>1. \quad (16)$$

Where,

ETx-- Energy for Transmitter

ERx-- Energy for Receiver

EDa – Energy for Data aggregation

Transmit amplifier

In this model, each node is allotted an initial energy value of 1Joule. Due to energy loss from data transmission or reception, a node has "failed" when its energy level drops below 0. After the underlying a round can begin

A tree structure is formed and a root node is selected.

## 4. Simulation Results and Discussions

ISSN: 2233-7857 IJFGCN

The ns-2.33 Network Simulator is used for the experimental investigation of the proposed MTF-DOSADF framework and its benchmarked ET-HDOSDF, IRA-DOSDF, and EGR-DOSDF frameworks. The simulation area considered for investigation is 1200x1200 square metres in which there is a random distribution of 200 sensor nodes across the entire network. With a transmission range of 35 metres, the sensing range of the sensor nodes is considered to be 30 metres. 5 Joules is the energy of each individual sensor node. Furthermore, in the comparative investigation of the proposed MTF-DOSADF framework with its benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks, the simulation setup considered is highlighted in Table 1.

**Table 1** Simulation Setup used for implementing the proposed MTF-DOSADF Framework

| Simulation parameters | Values |
|---|---|
| Number of sensor nodes | 200 |
| Simulation area | 1200x1200 square meters |
| Transmission range | 35 meters |
| Channel bandwidth | 1 Mbps |
| Propagation mode | Free space |
| Initial energy of node | 5J |
| Simulation time | 600 seconds |
| Packet size | 512 bytes |
| Node placement | Random deployed |

The predominance of the MTF-DOSADF Framework is initially compared with the benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks in this experimental investigation, using the packet dissemination rate, energy consumption, packet latency and reliable detection rate by varying the sensor nodes in the network. Figure 2 highlights the results of the proposed MTF-DOSADF framework, quantified by varying the number of network sensor nodes in terms of packet dissemination rate.

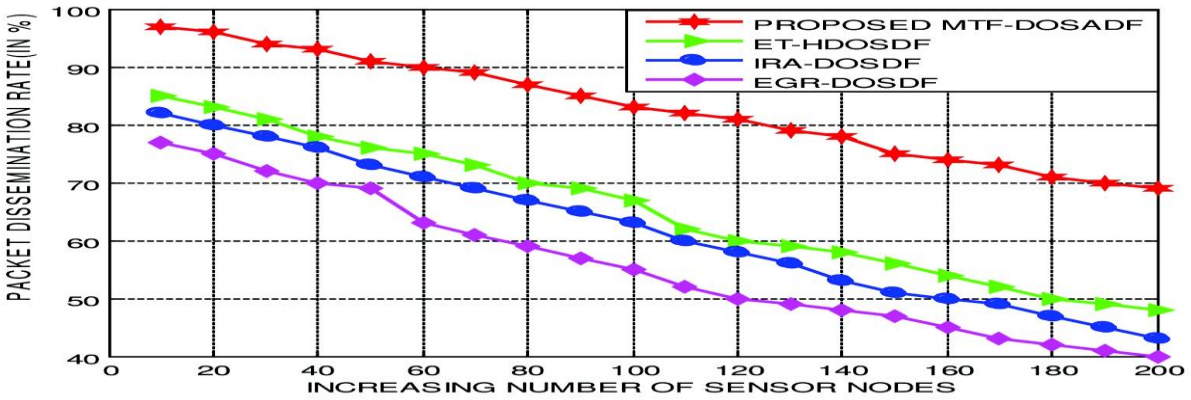


**Figure 2** MTF-DOSADF-packet dissemination rate under increasing sensor nodes

ISSN: 2233-7857 IJFGCN

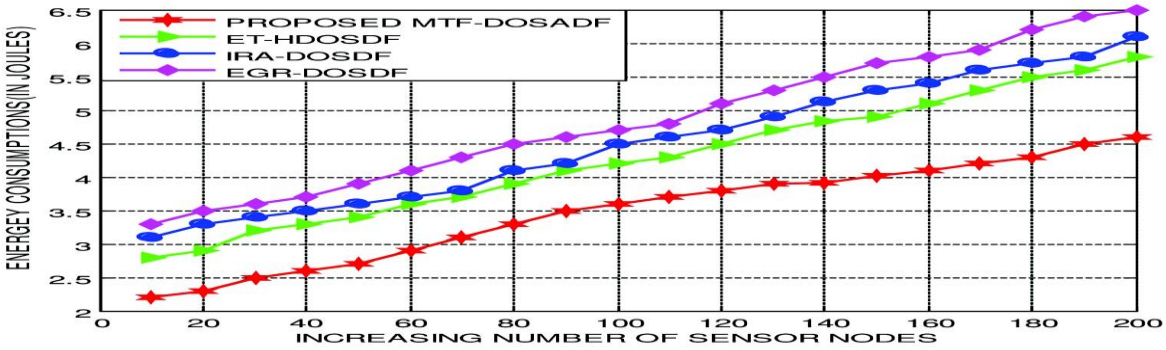


**Figure 3** MTF-DOSADF-energy consumptions under increasing sensor nodes

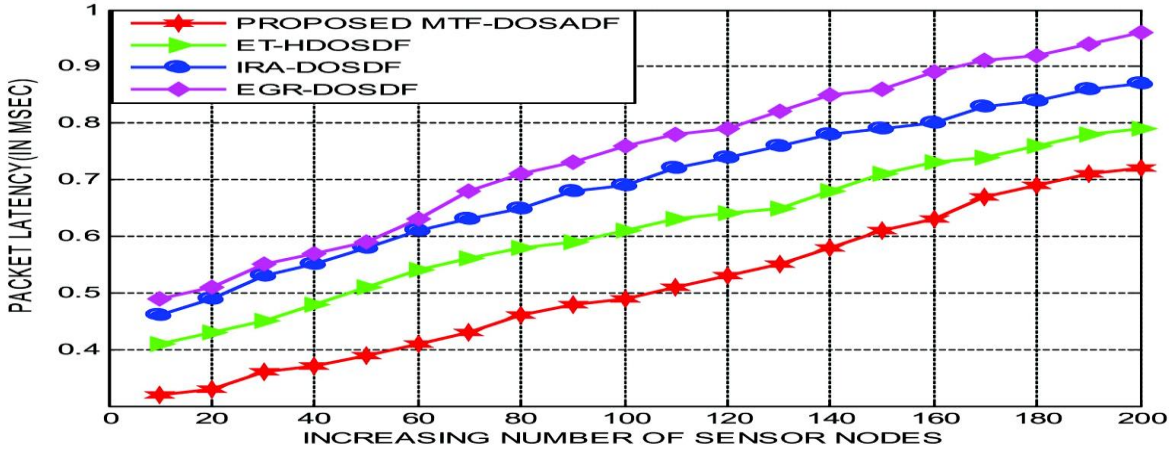


**Figure 4** MTF-DOSADF-packet latency under increasing sensor nodes

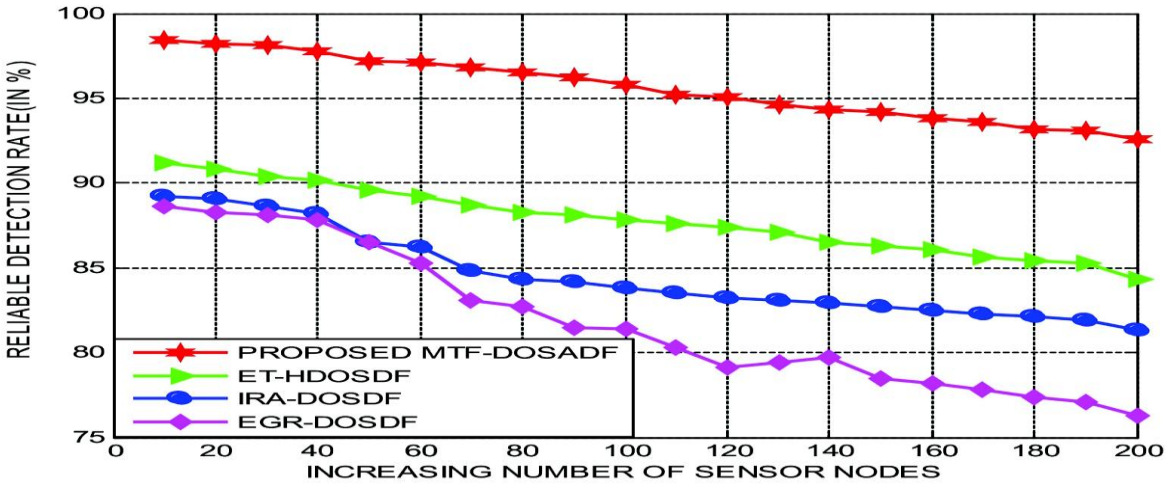


**Figure 5** MTF-DOSADF-Reliable detection rate under increasing sensor nodes

ISSN: 2233-7857 IJFGCN

In the proposed MTF-DOSADF framework, the packet dissemination rate is estimated to range from 98 percent to 69 percent, when the number of sensor nodes varies from 10 to 200 in monotonically increasing increments of 10. The packet dissemination rate of the benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks is between 86%-48%, 82%-45% and 77%-40%, respectively, in this context. Thus, compared to the benchmarked schemes used for analysis, the packet dissemination rate was determined to be improved by an average of 15%, 18% and 21%. This improvement in the proposed MTF-DOSADF framework is estimated primarily as a result of the extraction of contextual parameters which help to compute the reliability of the collaborative sensor nodes. The results of the proposed MTF-DOSADF framework, quantified in terms of energy consumption by varying the number of network sensor nodes, are shown in Figure 3. The graphs concluded that the proposed MTF-DOSADF framework's energy consumption is 3.3-6.5 Joules, ET-HDOSDF is 3.1-6.1 Joules, IRA-DOSDF is 2.8-5.8 Joules, and EGR-DOSDF is 2.3-4.7 Joules. It is therefore confirmed that the mean energy consumption of the proposed MTF-DOSADF framework is reduced by a margin of 1.1 Joules. This outstanding rate of reduction in the proposed MTF-DOSADF framework is facilitated by the use of energy as one of the parameters in the contextual reputation factor estimation during implementation. Figure 4 illustrates the packet latency plots of the proposed MTF-DOSADF framework by varying the number of network sensor nodes. The graphs concluded that the packet latency of the proposed MTF-DOSADF framework is between 0.48-0.97 milliseconds with an increasing number of 10 to 200 sensor nodes in increments of 10. However, the packet latency of the compared frameworks ET-HDOSDF, IRA-DOSDF and EGR-DOSDF are respectively 0.46-0.87 milliseconds, 0.41-0.79 milliseconds and 0.18-0.72 milliseconds. The packet latency of the proposed MTF-DOSADF framework has therefore been shown to decrease by a 23 percent margin compared to the baseline approaches used for analysis. This significant decrease in the packet latency of the proposed MTF-DOSADF framework is mainly due to the rapid process of detection of malicious nodes that has been ensured during the potential isolation process. The reliable detection rate of the proposed MTF-DOSADF framework analysed by varying the number of network sensor nodes is unveiled in Figure 5.

In addition, the predominance of the MTF-DOSADF framework is compared to the benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks using the rate of packet dissemination and energy consumption, by varying the number of malicious sensor nodes in the network that are selectively forwarded. In terms of packet dissemination rate, Figure 6 glorifies the results of the proposed MTF-DOSADF framework quantified by varying the number of selective forwarding malicious sensor nodes in the network. Compared to the existing frameworks, the packet dissemination rate of the proposed MTF-DOSADF Framework is set to be improved by 13 percent, 16 percent and 18 percent. Similarly, Figure 7 shows the results of the proposed MTF-DOSADF framework, quantified in terms of energy consumption, as determined by the number of malicious sensor nodes in the network being selectively forwarded. Compared with the existing frameworks, energy consumption was estimated to be reduced by 15 percent, 18 percent and 21 percent. This improvement rate in the dissemination rate of packets and the predominant reduction in energy consumption under the varying number of selective malicious nodes is mainly facilitated by the adaptive determination of the quantification parameter of availability.

In addition, by varying the number of hello flooding attacker nodes within the network, the significance of the MTF-DOSADF framework is compared with the benchmarked ET-HDOSDF, IRA-DOSDF, and EGR-DOSDF frameworks using packet dissemination rate and power consumption. Figure 8 shows the results of the proposed MTF-DOSADF framework quantified by varying the number of hi-flooding attacker nodes in the network in terms of packet dissemination rate. Under different hello flooding attacker nodes, the packet dissemination rate of the proposed MTF-DOSADF framework is determined to be improved by 11 percent, 13 percent and 16 percent compared to the existing frameworks. Similarly , Figure 9 exemplifies the results of the proposed MTF-DOSADF framework

ISSN: 2233-7857 IJFGCN

quantified by varying the number of attacker nodes in the network in terms of energy consumption. Compared to the existing frameworks, energy consumption was estimated to be minimised by 13 percent, 15 percent and 21 percent. This increase in the rate of packet dissemination and the predominant decrease in energy consumption under the varying number of hello flood attacker nodes is mainly facilitated by the flexible estimation of the availability factor that assists in the decision-making process.

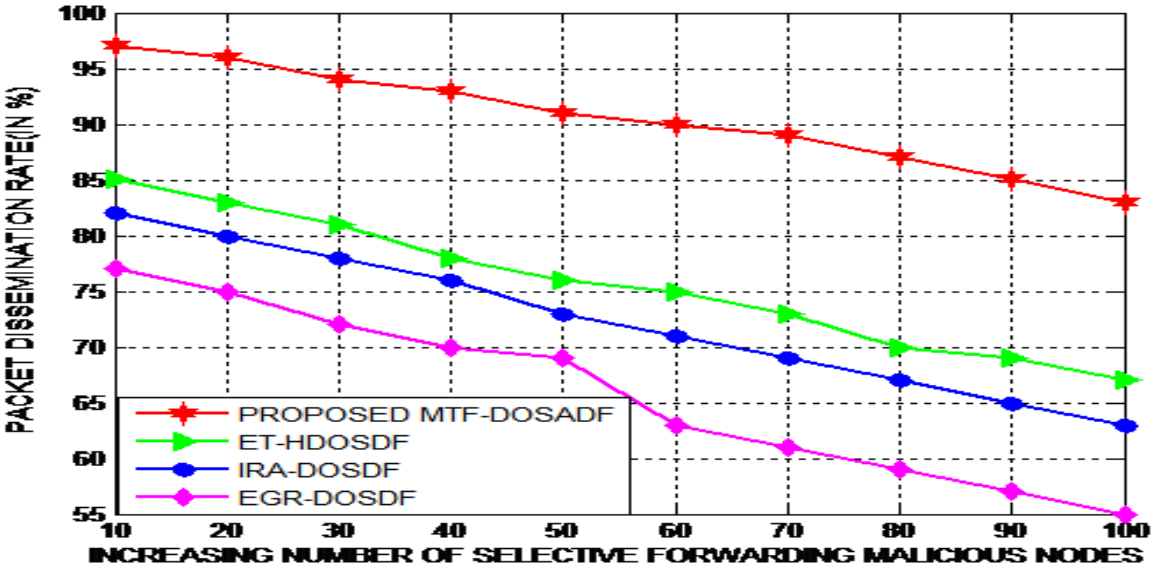


**Figure 6** MTF-DOSADF-packet dissemination rate-selective forwarding malicious nodes

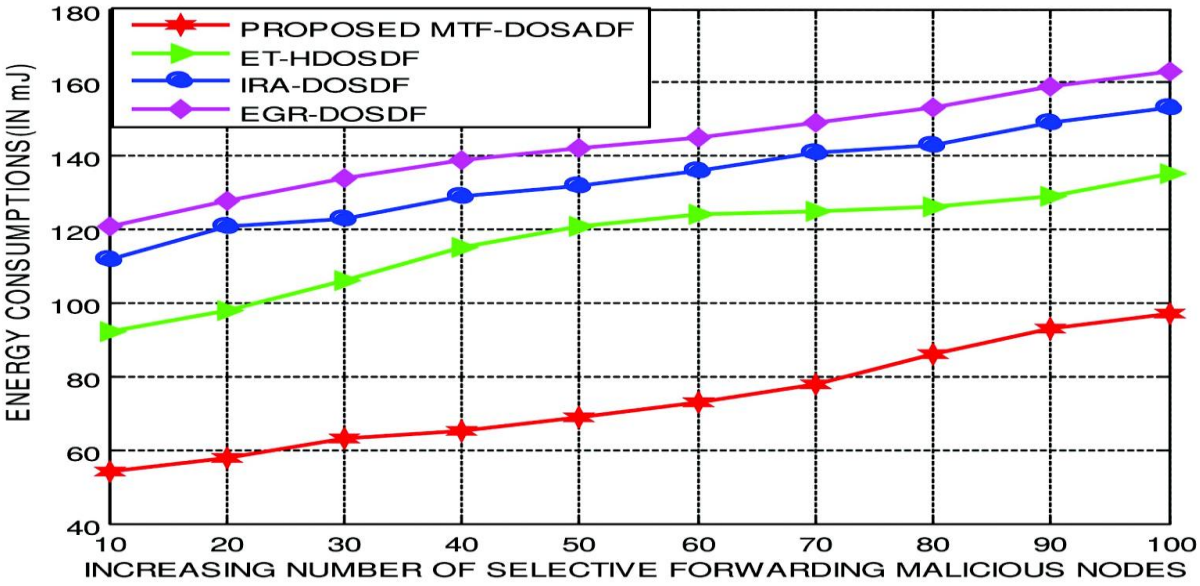


**Figure 7** MTF-DOSADF-energy consumptions-selective forwarding malicious nodes

ISSN: 2233-7857 IJFGCN

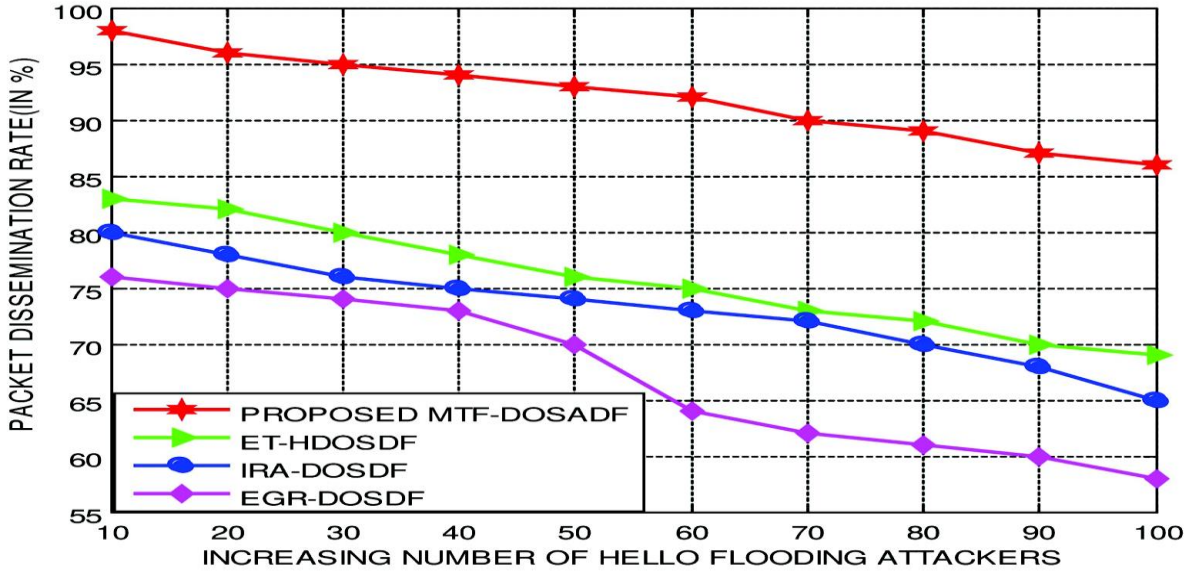


**Figure 8** MTF-DOSADF-packet dissemination rate-hello flooding attacker nodes

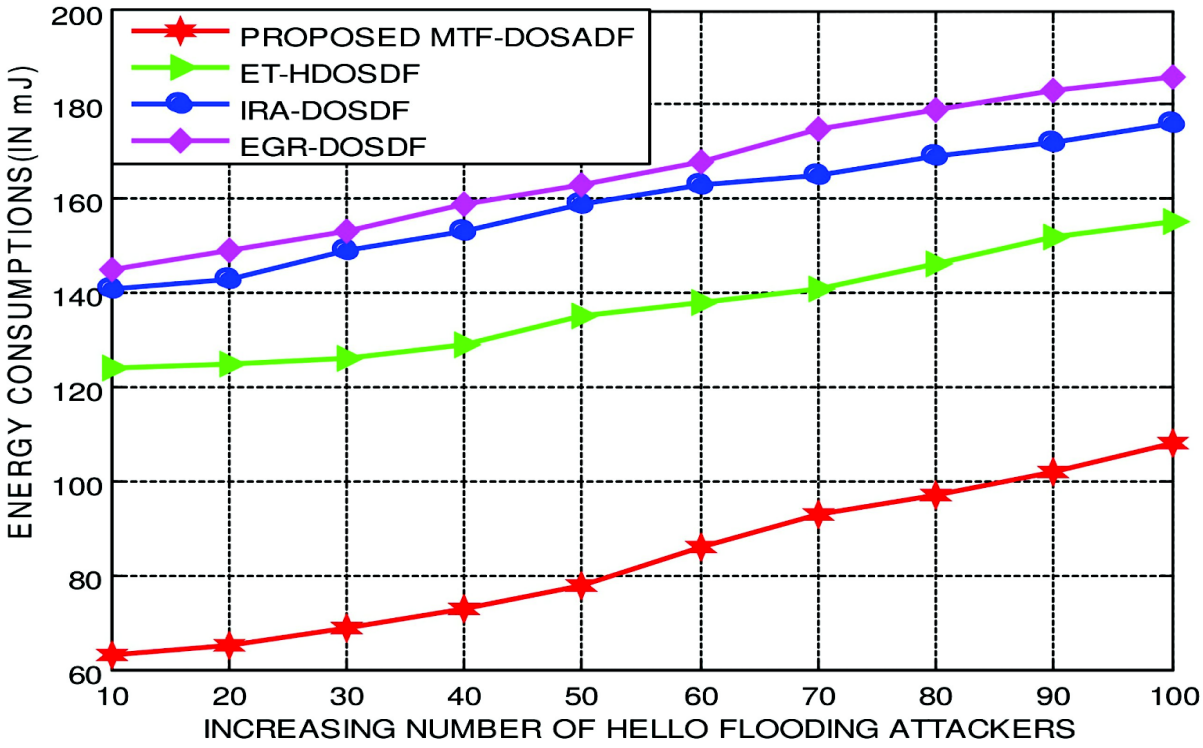


**Figure 9** MTF-DOSADF-energy consumptions under increasing hello flooding attackers

ISSN: 2233-7857 IJFGCN

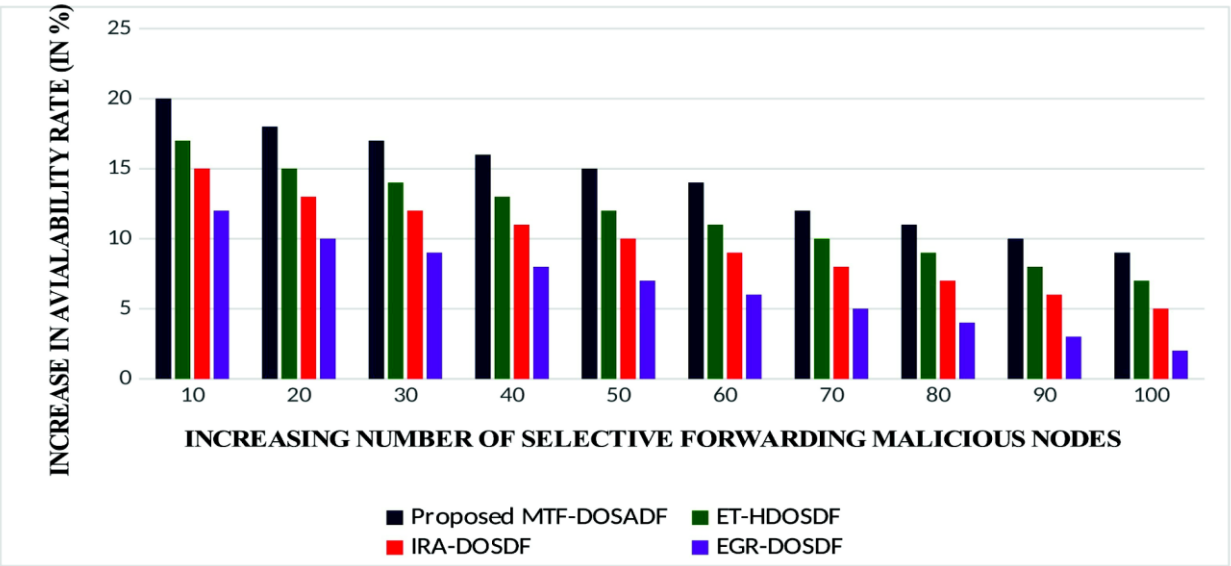


**Figure 10** MTF-DOSADF-Percentage Increase in Availability under increasing selective forwarding malicious nodes

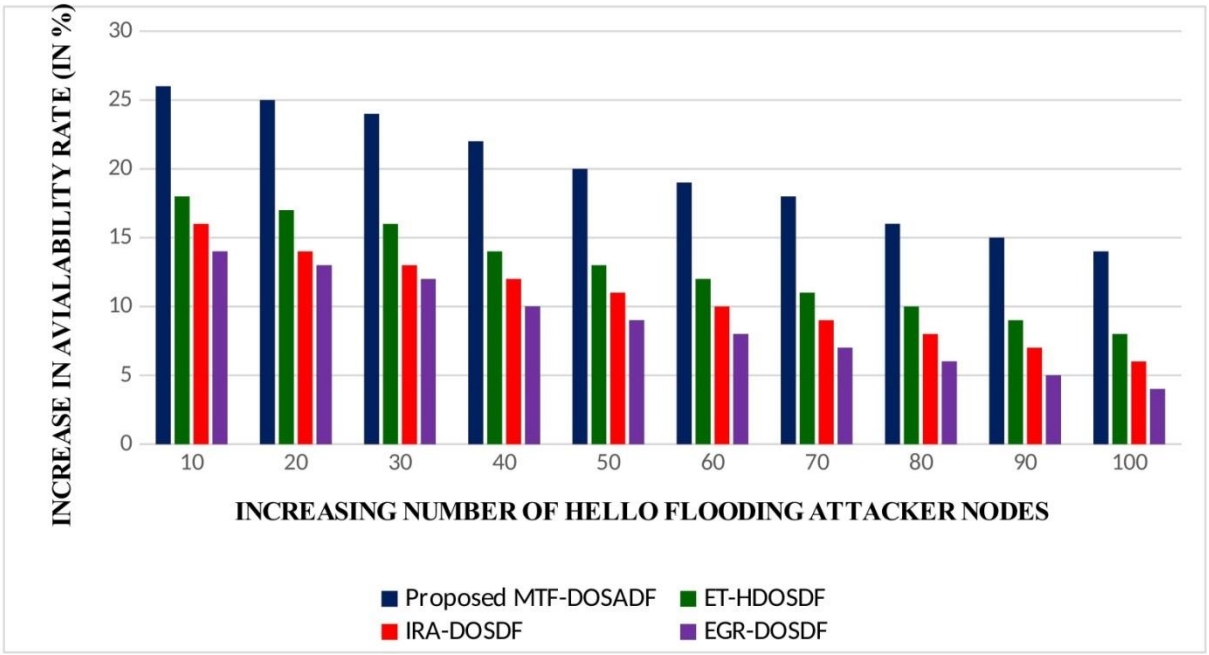


**Figure 11** MTF-DOSADF-Percentage Increase in Availability under increasing hello flooding attacker nodes

ISSN: 2233-7857 IJFGCN

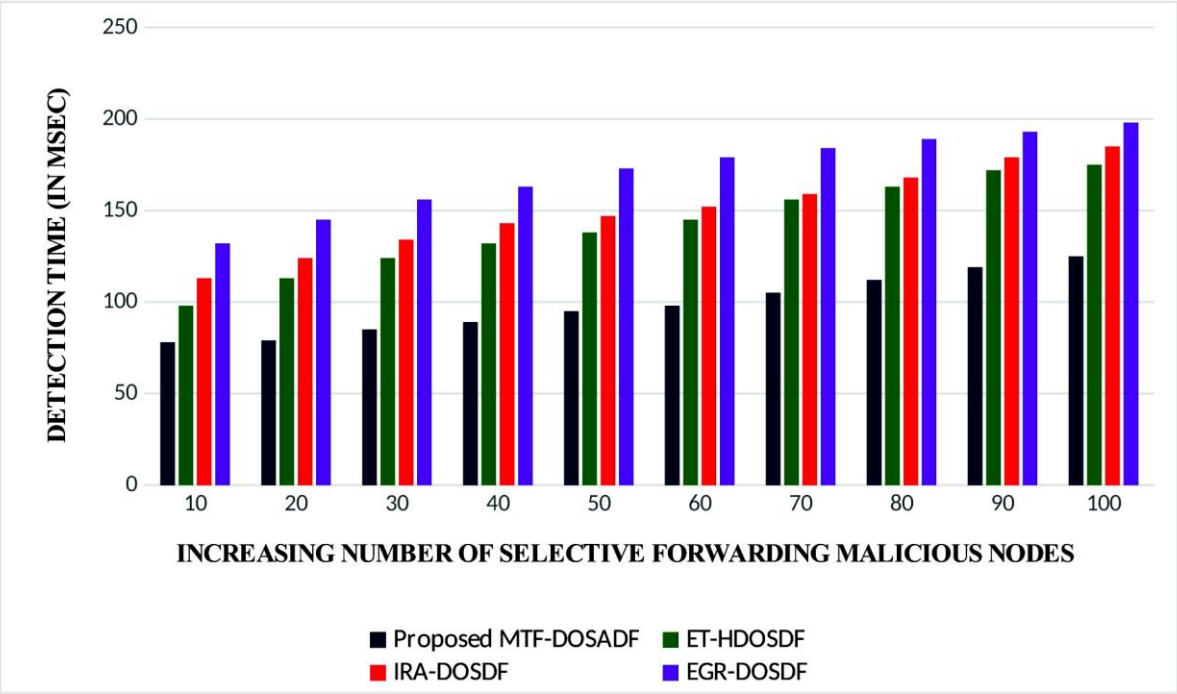


**Figure 12** MTF-DOSADF-Detection Time under increasing selective forwarding malicious nodes

ISSN: 2233-7857 IJFGCN

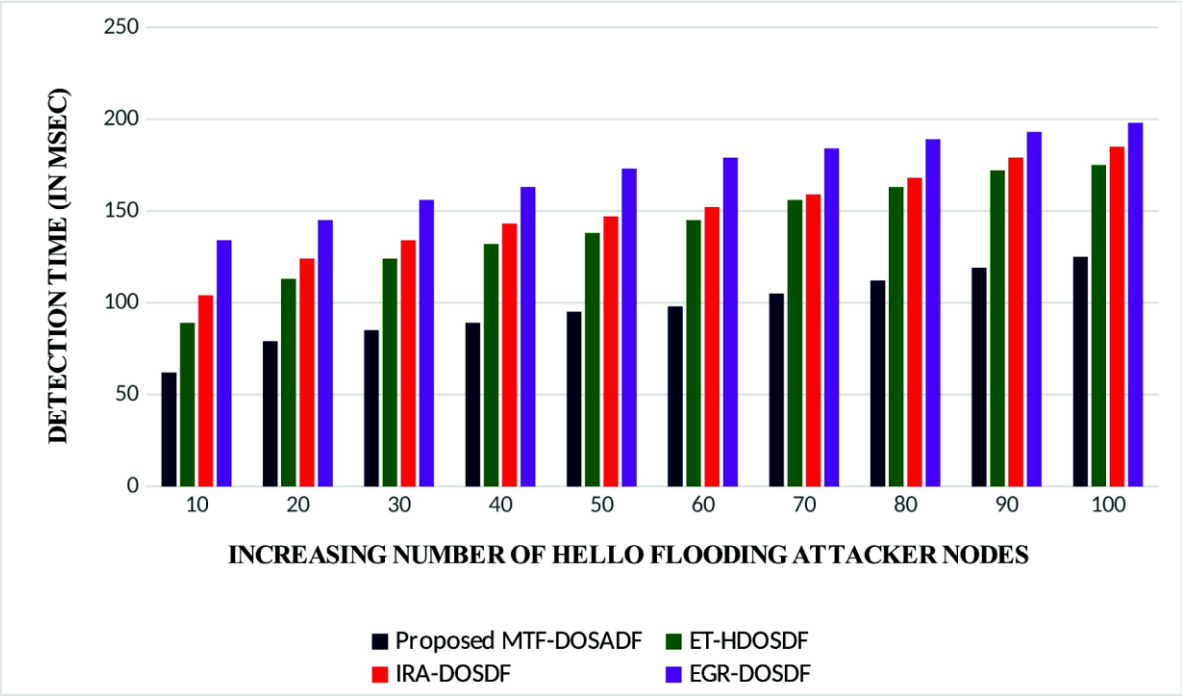


**Figure 13** MTF-DOSADF-Detection Time under increasing hello flooding attacker nodes

Finally, Figures 10 and 11 show the predominance of the proposed MTF-DOSADF evaluated with the increasing number of selective forwarding malicious nodes and hello flooding attacker nodes as a percentage increase in availability quantified. Compared to the benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks, the percentage increase in availability under increasing selective malicious forwarding nodes is determined to be improved by 8 percent, 12 percent and 15 percent. Compared to the benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks, the percentage increase in availability under increasing hello flood attacker nodes is determined to be improved by 10 percent, 13 percent and 18 percent. Similarly, Figures 12 and 13 show the potential of the proposed MTF-DOSADF quantified with a corresponding increase in the number of hello flood attacker nodes in terms of detection time. Compared to the benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks, the percentage decrease in detection time under increasing selective malicious forwarding nodes is determined to be minimised by 11 percent, 14 percent and 18 percent. Compared with the benchmarked ET-HDOSDF, IRA-DOSDF and EGR-DOSDF frameworks, the percentage decrease in detection time under increasing hello flood attacker nodes is determined to be reduced by 13 percent, 16 percent and 21 percent.

## 5. Conclusions

This suggested MTF-DOSADF was presented as the reliable attempt to detect and isolate the selective forwarding and hello flooding attack of the network's type of malicious intent. This proposed MTF-DOSADF incorporates the multi-perspective network parameter extraction phenomenon for selective forwarding attack handling and the projected availability factor for hello flooding attack mitigation. A predominant mean improvement of 18 percent in the packet dissemination rate, 22 percent in the detection rate and 17 percent and 15 percent in the energy consumption and packet latency of the network was confirmed by the simulation experiments of the proposed MTF-DOSADF studied under an

ISSN: 2233-7857 IJFGCN

increasing number of sensor nodes. A predominant increase of 16 percent in packet dissemination rate and 22 percent reduction in energy consumption was confirmed by the proposed MTF-DOSADF investigated under an increasing number of selective forwarding malicious nodes. Similarly, under an increasing number of hello flooding attacker nodes, the proposed MTF-DOSADF investigated proved a predominant 20 percent increase in packet dissemination rate and 17 percent reduction in energy consumption. It was estimated that the mean availability rate of the proposed MTF-DOSADF was maximized by 14 percent with a 17 percent reduction in detection time compared to the baseline detection frameworks considered for investigation.

**Funding**

Not applicable

**Conflict of interest**

The authors declare that there is no conflict of interest regarding the publication of this article.

## References

1. Kaplantzis, S., Shilton, A., Mani, N., &Sekercioglu, Y. A. (2007). Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines. 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 1(1), 23-34.
2. Wang, Y., & Li, G. R. (2012). Research on Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks. Advanced Materials Research, 433-440(1), 5298-5302.
3. Gavrić, Ž.,&Simić, D. (2018). Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. *Ingeniería e Investigación, 38*(1), 130-138.
4. Erdene-Ochir, O., Minier, M., Valois, F., &Kountouris, A. (2010). Toward Resilient Routing in Wireless Sensor Networks: Gradient-Based Routing in Focus. 2010 Fourth International Conference on Sensor Technologies and Applications, 1(1), 34-45.
5. Brown, J., & Du, X. (2008). Detection of Selective Forwarding Attacks in Heterogeneous Sensor Networks. 2008 IEEE International Conference on Communications, 1(1), 45-57.
6. He, Z., & Voigt, T. (2013). Droplet: A New Denial-of-Service Attack on Low Power Wireless Sensor Networks. 2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, 1(1), 65-78.
7. Saghar, K., Kendall, D., & Bouridane, A. (2015). RAEED: A solution for hello flood attack. *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 1*(1), 56-67.
8. Saghar, K., Farid, H., Kendall, D., & Bouridane, A. (2016). Formal specifications of Denial of Service attacks in Wireless Sensor Networks. 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 1(2), 35-47.
9. Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2017). A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks. Australian Journal of Telecommunications and the Digital Economy, 5(1), 50.
10. Airehrour, D., Guttierrez, J., & Ray, S. K. (2018). A Trust-based Defence Scheme for Mitigating Blackhole and Selective Forwarding Attacks in the RPL Routing Protocol. Australian Journal of Telecommunications and the Digital Economy, 6(1), 41-59.
11. Fu, X., Li, P., & Wu, J. (2013). Detection and defense scheme for selective forwarding attacks in wireless sensor network. *Journal of Computer Applications*, *32*(10), 2711-2715.

ISSN: 2233-7857 IJFGCN

12. Hassoubah, R. S., Solaiman, S. M., & Abdullah, M. A. (2015). Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme. International Journal of Computer and Communication Engineering, 4(3), 156-165.
13. Ranjith H.D, Mayur. S. (2015). Security Enhancement on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme. International Journal of Innovative Research in Science, Engineering and Technology, 04(03), 34-46.
14. Alajmi, N., &Elleithy, K. (2015). Multi-Layer Approach for the Detection of Selective Forwarding Attacks. *Sensors*, *15*(11), 29332-29345.
15. Khosravi, H., Azmi, R., &Sharghi, M. (2016). Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks. *International Journal of Future Computer and Communication*, *5*(2), 99-103.
16. Arivanantham, P., &Ramakrishnan, M. (2017). Enhanced Detective Approach for Selective Forwarding Attacks in Wireless Sensor Networks. *Journal of Computational and Theoretical Nanoscience*, *14*(8), 3807-3811.
17. Chawla, P., &Sachdeva, M. (2017). Detection of Selective Forwarding (Gray Hole) Attack on LEACH in Wireless Sensor Networks. *Advances in Intelligent Systems and Computing*, *1*(1), 389-398.
18. Mehetre, D. C., Roslin, S. E., &Wagh, S. J. (2018). Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Cluster Computing, 1(1), 78-92.
19. Jinhui, X., Yang, T., Feiyue, Y., Leina, P., Juan, X., & Yao, H. (2018). Intrusion Detection System for Hybrid DoS Attacks using Energy Trust in Wireless Sensor Networks*. *Procedia Computer Science*, *131*(1), 1188-1195.
20. Ji, Y. (2018). A Wireless Sensor Network-Based Defence Model against Selective Forwarding Attack. *International Journal of Online Engineering (iJOE)*, *14*(05), 70.

ISSN: 2233-7857 IJFGCN